Claims

1. A security module within a printer that is operable to:

receive a message from an attached computer requesting a secure printing key;

generate a key in response to the received message; and

send the key to the attached computer requesting the key.

2. The security module of claim 1, wherein the generated key comprises a symmetric encryption key.

3. The security module of claim 2, wherein the sending the key to the attached computer requesting the key comprises sending the key to the attached computer over a secured connection.

4. The security module of claim 1, wherein the symmetric key is a DES key.

5. The security module of claim 1, wherein generating a key comprises generating a public key and a private key, and wherein sending the key to the attached computer requesting the key comprises sending the public key to the attached computer requesting the key.

6. The security module of claim 5, wherein the public key is sent to the attached computer over a secured connection.

7. The security module of claim 1, wherein the security module receives the message from an attached computer via a web server hosted within the printer.

8. The security module of claim 1, wherein the security module executes within a Java virtual machine within the printer.

9. The security module of claim 1, wherein the attachment between the printer and the attached printer is a network attachment.

10. A machine-readable medium with instructions stored thereon, the instructions when executed operable to cause a computerized printer to:

receive a message from an attached computer requesting a secure printing key;

generate a key in response to the received message; and

send the key to the attached computer requesting the key.

11. The machine-readable medium of claim 10, wherein the generated key comprises a symmetric encryption key.

12. The machine-readable medium of claim 11, wherein the sending the key to the attached computer requesting the key comprises sending the key to the attached computer over a secured connection.

13. The machine-readable medium of claim 10, wherein the symmetric key is a DES key.

14. The machine-readable medium of claim 10, wherein generating a key comprises generating a public key and a private key, and wherein sending the key to the attached computer requesting the key comprises sending the public key to the attached computer requesting the key.

15. The machine-readable medium of claim 14, wherein the public key is sent to the attached computer over a secured connection.

16. The machine-readable medium of claim 10, wherein the security module receives the message from an attached computer via a web server hosted within the printer.

17. The machine-readable medium of claim 10, wherein the security module executes within a Java virtual machine within the printer.

18. The machine-readable medium of claim 10, wherein the attachment between the printer and the attached printer is a network attachment.

19. A peripheral device module executable within the computerized peripheral device that when executed is operable to:

receive a message from an attached computer requesting a secure printing key;

generate a key in response to the received message; and

send the key to the attached computer requesting the key.

20. A computer printer system, comprising:

receive a message from an attached computer requesting a secure printing key;

generate a key in response to the received message; and

send the key to the attached computer requesting the key.

21. A method of managing a printer in a computerized system external to the printer, comprising:

receive a message from an attached computer requesting a secure printing key;

generate a key in response to the received message; and

send the key to the attached computer requesting the key.